## REMARKS/ARGUMENTS

Claims 1-11, 13-22, 26, 27, and 30-32 are pending. Claims 1, 2, 16, 17, 26, 27, 30, 31, and 32 have been amended. Claims 12, 28, 29, 33, and 34 have been canceled. No new matter has been added.

Claims 1, 9-17, 26-30, and 32 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ohran in view of Yanai et al. Applicants traverse the rejection. Claim 1 is directed to a method of controlling security of data in a storage system having a local disk system and a remote disk system that are coupled to at least one host computer. The local and remote disk systems are "intelligent" storage systems including a plurality of storage volumes (see Fig. 1). The local disk system has first and second volumes of storage that are associated with first and second encryption keys, respectively. That is, the data stored in the first volume is encrypted using the first key and the data stored in the second volume is encrypted using the second key. As a result, the data of a first user who is assigned to the first volume and the data of a second user who is assigned to the second volume can be managed using different encryption keys. Ohran does not disclose an "intelligent" storage system nor the concept of associating different encryption keys to the different storage volumes. Yanai does not remedy these deficiency of Ohran. Claim 1 is allowable at least for this reason.

Claim 9 is directed to a method for changing an encryption key while operating a storage system having a local disk system and a remote disk system. The method includes storing an encryption key in a memory in the local disk system. The encryption key is transmitted to the remote disk system and storing it in a memory there via a first communication link coupling the local and remote disk systems. A boundary for use of the encryption key is determined by the local disk system. The boundary defines which data are to be encrypted using the encryption key. The determined boundary is received from the local disk system by the remote disk system. In both the local and the remote disk systems, determining a relationship of present operations to the boundary by each of the local and remote disk systems. In both the local and the remote disk systems, waiting for the boundary and then changing the encryption key for data stored thereafter by each of the local and remote disk systems. Neither Ohran nor

Yanai discloses or suggest the method of dynamically changing the encryption key by using the boundary, in the manner recited. Claim 9 is allowable at least for this reason. Claim 13 discloses the use of boundary. Claim 13 is allowable at least for this reason.

Claim 16 is directed to a method for controlling encryption in a storage system. The claim recites, "storing first and second encryption keys in a memory in the local disk system that is coupled to a host computer via a first communication link, the first and second encryption keys assigned to first and second volumes of the local disk system, respectively; transmitting via a second communication link the first and second encryption key to the remote disk system and storing it in a memory there, the remote disk system including third and fourth volumes corresponding to the first and second volume, respectively." Neither Ohran nor Yanai discloses or suggests the first and second encryption keys assigned to the first and second volumes, in the manner recited. Claim 16 is allowable.

Claim 17 is directed to a storage system. The claim recites, "a local disk system including a plurality of volumes of media for storing data, said local disk system being coupled to a host computer via a first communication link to enable the host computer to access said volumes, the plurality of volumes in the local disk system including first and second volumes that are associated with first and second encryption keys, respectively...wherein the local disk system determines whether encryption is to be employed in the data associated with the first volume in the local disk system, and if so, the local disk system encrypts the data to be transferred to the remote disk system using the first key..." Neither Ohran nor Yanai discloses or suggests the first and second encryption keys assigned to the first and second volumes, in the manner recited. Claim 17 is allowable.

Claim 26 is directed to a storage system and recites, "a local memory in the local disk system for storing a first encryption key assigned to a first volume in the local disk system and a second encryption key assigned to a second volume in the local disk system." Neither Ohran nor Yanai discloses or suggests the first and second encryption keys assigned to the first and second volumes, in the manner recited. Claim 26 is allowable.

Claim 27 is directed to a method for controlling security of data in a storage system, where the local disk system includes first and second volumes that are assigned first and second encryption keys, respectively. Neither Ohran nor Yanai discloses or suggests the first and second encryption keys assigned to the first and second volumes, in the manner recited. Claim 27 is allowable.

Claim 30 is directed to a storage system and recites, "a local disk system including first and second storage volumes for storing data, the first and second volumes being assigned with first and second encryption keys, respectively, wherein the local disk system is connected to a host computer via a first communication link." Neither Ohran nor Yanai discloses or suggests the first and second encryption keys assigned to the first and second volumes, in the manner recited. Claim 30 is allowable.

Claim 32 is directed to a method of controlling security data in a disk system. The method recites, "at the disk system, receiving data to be stored from the host computer via a first communication link, so that the data can be stored in a given area in the disk system, the disk system including first and second volume that are assigned first and second encryption keys, respectively,; encrypting the data received from the host computer using the first or second key according to the location of the given area, wherein the first key is used if the given area in the first volume and the second key is used if the given area is in the second volume, the encrypting performed by the disk system." Neither Ohran nor Yanai discloses or suggests the first and second encryption keys assigned to the first and second volumes and the use of the first and second keys, in the manner recited. Claim 32 is allowable.

Claims 2-8, 18-22, 31, 33, and 34 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ohran in view of Yanai et al. and further in view of Jacobson. Applicants traverse the rejection. Claim 2 recites, "maintaining an encryption control table on the local disk system, the encryption control table including a list of encryption keys for selected volumes of the local and the remote disk system, wherein the data transfer between the local disk system and the remote disk system occurs via a communication link that couples the local disk system to the remote disk system, so that the local disk system may send the data to the remote disk system

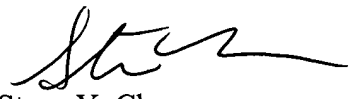
without direct involvement from the host computer, wherein the list of encryption keys includes the first and second keys, the first key being assigned to a first set of volumes in the local disk system, and the second key being assigned to a second set of volumes in the local disk system, each of the first and second set of volumes including one or more volumes, wherein the retrieving step includes accessing the encryption control table to obtain an appropriate encryption key, where the data are encrypted using the first key if the data to be transferred to the remote disk system are associated with the first set of volumes and encrypted using the second key if the data to be transferred to the remote disk system are associated with the second set of volumes, wherein the remote disk system is coupled to a second host computer." None of the cited references discloses or suggests the above recited features. Claim 2 is allowable. Claim 3-8 depend from claim 2 and are allowable at least for this reason. Claims 18-22 depend from claim 17 and are allowable at least for this reason. Claim 31 depends from claim 30 and is allowable at least for this reason. Claims 33 and 34 have been canceled.

## CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,



Steve Y. Cho
Reg. No. 44,612

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
Attachments
SYC:srb
60607062 v1